PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-345819

(43)Date of publication of application : 14.12.2001

(51)Int.Cl. H04L 12/28
H04Q 7/38
H04L 9/32

(21)Application number : 2000-164519

(22)Date of filing : 01.06.2000

(71)Applicant : SHARP CORP

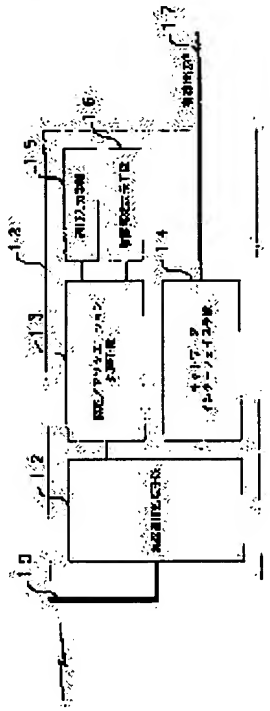
(72)Inventor : KIMURA SHINYA

(54) ACCESS POINT DEVICE AND METHOD OF AUTHENTICATION PROCESSING THEREFOR

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an access point device and a method of authentication processing therefor, with which a security level can be remarkably improved, in a wireless LAN system.

SOLUTION: An access point device 18 is provided with an authentication request display means 16 for making the access point device 18 report the existence of a mobile station requesting authentication for obtaining the final permission of an authentication procedure inside an area, to a network manager for managing a LAN, when the mobile station inside the area is to perform the authentication procedure, before the start of an association procedure and an authentication input means 15 for the network manager, who receives the notice, to instruct the permission of refusal of authentication to the mobile station requesting authentication.



LEGAL STATUS

[Date of request for examination] 19.07.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3585422

[Date of registration] 13.08.2004

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3585422号
(P3585422)
(45)発行日　平成16年11月4日(2004.11.4)　(24)登録日　平成16年8月13日(2004.8.13)

(51)Int.Cl.[7]　F I
H04L 12/28　H04L 12/28　300Z
H04L 9/32　H04B 7/26　109R
H04Q 7/38　H04L 9/00　673A
H04L 9/00　675A

請求項の数 6　(全 12 頁)

(21)出願番号　特願2000-164519(P2000-164519)
(22)出願日　平成12年6月1日(2000.6.1)
(65)公開番号　特開2001-345819(P2001-345819A)
(43)公開日　平成13年12月14日(2001.12.14)
審査請求日　平成14年7月19日(2002.7.19)

(73)特許権者　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町２２番２２号
(74)代理人　100091096
弁理士　平木　祐輔
(72)発明者　木村　真也
大阪府大阪市阿倍野区長池町２２番２２号
シャープ株式会社内

審査官　石井　研一

最終頁に続く

(54)【発明の名称】アクセスポイント装置及びその認証処理方法

1

(57)【特許請求の範囲】
【請求項１】有線伝送路で構築されるネットワークとのインターフェース機能を備え、無線ＬＡＮエリア内で複数の移動局とデータリンク接続を行うアクセスポイント装置において、
複数の移動局とのデータリンク確立を行うためのアソシエーション手順と認証手順を実行する認証／アソシエーション実行手段と、
前記エリア内の移動局が、前記アソシエーション手順を開始する前に前記認証手順を行おうとする場合に、前記ＬＡＮを管理するネットワーク管理者に対し、認証手順の最終的な許可を得るために、認証を求めている移動局がいることを通知する通知手段と、
前記通知を受けた前記ネットワーク管理者による、前記認証を求めている移動局に対しての認証の許可又は拒否

2

の指示が入力される入力手段と、
を備えることを特徴とするアクセスポイント装置。
【請求項２】前記通知手段は、前記ネットワーク管理者に対して、前記認証手順の最終的な許可を通知するとともに、最終認証が行われるまでの最大待ち時間を設定した認証待ちタイマをスタートし、
前記認証待ちタイマがタイムアウトする前に、前記ネットワーク管理者による、前記認証を求めている前記移動局に対しての認証の許可の指示が入力されたとき、認証応答メッセージを、認証許可として前記移動局に返信することを特徴とする請求項１記載のアクセスポイント装置。
【請求項３】有線伝送路で構築されるネットワークとのインターフェース機能を備え、無線ＬＡＮエリア内で複数の移動局とデータリンク接続を行うアクセスポイント

3

装置の認証処理方法において、
前記移動局から前記アクセスポイント装置への認証要求により、前記移動局及び前記アクセスポイント装置が、所定の認証手続を開始する第１ステップと、
前記認証手続により、前記アクセスポイント装置が、前記移動局への認証を許可しようとするとき、前記認証手続における最終メッセージである認証応答メッセージを前記移動局に返信する前に、前記ＬＡＮを管理するネットワーク管理者に対して、前記認証手順の最終的な許可を通知するとともに、最終認証が行われるまでの最大待ち時間を設定した認証待ちタイマをスタートさせる第２ステップと、
前記ネットワーク管理者が、前記アクセスポイント装置に対して、前記認証待ちタイマがタイムアウトする前に、最終の認証の許可又は拒否を指示する第３ステップと、
前記ネットワーク管理者により、前記認証待ちタイマがタイムアウトする前に、最終の認証許可が指示されると、前記アクセスポイント装置が、前記認証応答メッセージを、認証許可として前記移動局に返信する第４ステップと、
前記認証応答メッセージを受信した前記移動局が、アソシエーションの手順を開始する第５ステップと、
を実行することにより前記移動局の認証が完了し、アソシエーション手順を開始する
ことを特徴とするアクセスポイント装置の認証処理方法。
【請求項４】前記第３ステップでは、前記ネットワーク管理者が、認証を拒否する指示を前記アクセスポイント装置に指示した場合に、前記認証応答メッセージを、認証拒否として前記移動局に返信する
ことを特徴とする請求項３記載のアクセスポイント装置の認証処理方法。
【請求項５】前記第３ステップでは、前記ネットワーク管理者が、認証を拒否又は許可する指示を前記アクセスポイント装置に指示する前に、前記認証待ちタイマがタイムアウトすると、前記認証応答メッセージを、認証拒否として前記移動局に返信する
ことを特徴とする請求項３記載のアクセスポイント装置の認証処理方法。
【請求項６】前記認証手続は、ＩＥＥＥ８０２．１１が規定するShared Key Authentication手順であることを特徴とする請求項３乃至５のいずれかに記載のアクセスポイント装置の認証処理方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、アクセスポイント装置及びその認証処理方法に関し、詳細には、無線を利用した、ワイヤレスＬＡＮシステムにおいて、悪意を持った侵入者の移動局からの

4

不正なアクセスを防止するためのアクセスポイント装置及びその認証処理方法に関する。
【０００２】
【従来の技術】
近年、インターネットの爆発的な普及に伴い、オフィス、家庭等で、ＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）を構築するケースが増えてきている。デジタル無線通信技術の進歩も手伝い、ケーブル配線の煩わしさから、無線でＬＡＮを構築する、いわゆるワイヤレスＬＡＮのニーズも非常に高まっており、さらに、ノート型パソコンに代表される移動端末での移動環境下における、使用が可能であることも手伝い、将来的には、かなりの数の普及台数が期待されている。このワイヤレスＬＡＮの代表的な技術としては、既に、ＩＥＥＥ（Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｅｌｅｃｔｒｉｃａｌ ａｎｄ Ｅｌｅｃｔｒｏｎｉｃｓ Ｅｎｇｉｎｅｅｒｓ）において、標準化されている、ＩＥＥＥ８０２．１１がある。この標準化された技術は、ＯＳＩモデルにおける、物理層から、データリンクの下位副層であるＭＡＣ（Ｍｅｄｉａ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ：媒体アクセス制御）層までを規定しており、有線のＬＡＮ伝送路である、イーサーネットと置きかえることができ、さらに、ワイヤレスであるが故の付加機能として、ローミング（ｒｏａｍｉｎｇ）機能も提供できる仕様になっている。
【０００３】
さて、有線のイーサーネット等で、ＬＡＮを構築する場合、ＬＡＮに接続することは、物理的に、ハブ等にケーブルを接続するため、データリンクレベルのセキュリティレベルは非常に高い。つまり、侵入者が、オフィス等に不正に侵入し、端末等をネットワークに接続しようと思っても、ケーブル接続という物理的な作業が必要であり、それを、密かに行うことは、一般的なＬＡＮの配置状況（特に、比較的中小規模のＬＡＮ）からして、非常に困難である。何故なら、そのＬＡＮの利用者と、そのＬＡＮを構成するハブやルーター等が、同一の居室内に存在するケースが殆どだからである。一方、ワイヤレスＬＡＮシステムの場合は、前記、イーサーネット等のケーブル接続の作業は、自動的なアソシエーション（Ａｓｓｏｃｉａｔｉｏｎ）手順により置き換わる。前記、既存のＩＥＥＥ８０２．１１等のシステムにおいて、このアソシエーション手順とは、移動端末が有線等のバックボーン・ネットワークに接続されているアクセスポイントに対して、自分自身の存在を認識してもらうための手順であり、この手順が完了すれば、データ通信を行うことができる。この手順においては、アクセスポイント（ａｃｃｅｓｓ ｐｏｉｎｔ）のカバーする有限エリアにいる移動端末は、前記アクセスポイントに対して、アソシエーションを行う前に、オプションの認証手続きをすることにより、データリンクレベルのセキュリティを

5

確保することになる。

【０００４】

このアソシエーション手順によれば、前記移動局は、アソシエーション要求を、前記アクセスポイントに対して行う場合、そのアソシエーション要求メッセージ中に、ＳＳＩＤ（Ｓｅｒｖｉｃｅ　Ｓｅｔ　Ｉｎｄｅｎｔｉｆｉｅｒ）を含ませ、これを受信したアクセスポイントは、前記ＳＳＩＤにて、前記移動局を識別し、予め決められたアソシエーション許可ルールに従い、そのアソシエーションを許可するかどうかを決定し、許可する場合は、アソシエーション許可の返信メッセージを、拒否する場合は、アソシエーション拒否の返信メッセージを、前記移動局に送信する。したがって、このアソシエーション手順だけでは、悪意を持ってネットワークに侵入しようとする者が、このＳＳＩＤさえ入手してしまえば、簡単にアソシエーションが可能になってしまう。それを避けて、本アソシエーション手順を実行するために、認証手続きを行うオプションが設けられている。つまり、認証手続きを行うオプションを設ける方式によれば、前記移動端末は、本認証手続きを完了しなければ、アソシエーションができないため、データ通信を開始することができず、これは、物理的な接続作業を必要としない、前記有限エリア内の、悪意を持った移動端末からの、不正なアソシエーションを防ぐ有効な機能を提供することになる。

【０００５】

ＩＥＥＥ８０２．１１においては、この認証手続きは、Ｓｈａｒｅｄ　Ｋｅｙ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ手順として定義されており、この手順を図５及び図６により説明する。　図５は、従来のワイヤレスＬＡＮシステムの概略構成を示す図、図６は、従来の認証手順とアソシエーション手順の制御シーケンスを示す図である。

【０００６】

図５において、１はワイヤレス・エリア・ネットワーク、２はアクセスポイントＡＰ、３は移動局ＭＴ１、４は移動局ＭＴ２、５は移動局ＭＴ３、６は移動局ＭＴ４、７はワイヤレス・エリア・ネットワーク１外の他ネットワークである。

【０００７】

ある有線伝送路により実現される、他ネットワーク７に接続されたアクセスポイントＡＰ２と、そのアクセスポイントＡＰ２がカバーする、有限なエリアに存在する、移動局ＭＴ１、ＭＴ２、ＭＴ３、ＭＴ４から構成されるワイヤレス・エリア・ネットワーク１において、ある移動局（例えば、ＭＴ１）が、電源を投入するなどの動作により、前記アクセスポイントＡＰ２に対して、アソシエーション前の認証手続きをする場合のシーケンスは、図６に示される。

【０００８】

6

まず、移動局ＭＴ１は、Ｓｈａｒｅｄ　Ｋｅｙ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ方法による認証手続きを開始するための、認証要求メッセージ１を、アクセスポイントＡＰ２に送信する。ＡＰ認証処理８（ＡＰ認証処理「１」）として、このメッセージを受信したＡＰ２は、この認証手続きの度に、任意に決めることができる、Ｉｎｉｔｉａｌｉｚａｔｉｏｎ　ＶｅｃｔｏｒとＳｅｃｒｅｔ　Ｋｅｙの値を、パラメータとし、ＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）ＰＲＮＧ（Ｐｓｅｕｄｏｒａｎｄｏｍ　Ｎｕｍｂｅｒ　Ｇｅｎｅｒａｔｏｒ）のアルゴリズムに従い数値演算を行い、１２８０ｃｔｅｔの、一意に決まるＣｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を算出し、この値を含めた認証応答メッセージ１を、移動局ＭＴ１に送信する。

【０００９】

次に、ＭＴ認証処理９（ＡＰ認証処理「２」）として、本認証応答メッセージ１を受信した移動局ＭＴ１は、その中含まれる前記Ｃｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を、ＷＥＰの暗号化アルゴリズムに従い、Ｓｈａｒｅｄ　Ｓｅｃｒｅｔ　Ｄａｔａと、Ｉｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒをパラメータに、暗号化を行い、その値を、前記Ｉｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒと共に、認証要求メッセージ２に含めて、前記アクセスポイントＡＰ２に返信する。

【００１０】

さらに、ＡＰ認証処理１０（ＡＰ認証処理「２」）として、本認証要求メッセージ２を受信した、アクセスポイントＡＰ２は、受信した暗号化されたＣｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を、同時に受信したＩｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒと、予め知っている前記Ｓｈａｒｅｄ　Ｓｅｃｒｅｔ　Ｄａｔａを基にデコードし、その結果と、前述の元のＣｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を比較し、それが同一であれば、認証許可とし、同一でなければ、認証拒否とし、その結果を認証応答メッセージ２として、移動局ＭＴ１に返信する。そこで、本認証応答メッセージ２を受信した移動局ＭＴ１は、その結果が、許可であれば、次のアソシエーションの手順に入ることができ、拒否の場合は、認証失敗ということで、アソシエーション手続きを行うことはできない。

【００１１】

ここでのアソシエーション処理は、前述の通り、移動局ＭＴ１からの、アソシエーション要求メッセージ中の、ＳＳＩＤ（Ｓｅｒｖｉｃｅ　Ｓｅｔ　Ｉｄｅｎｔｉｆｉｅｒ）を受信したアクセスポイントＡＰ２が、前記ＳＳＩＤにて、移動局を識別し、予め決められたアソシエーション許可ルールに従い、そのアソシエーションを許可するかどうかを決定し、許可する場合は、アソシエーション許可のアソシエーション応答メッセージを、拒否する場合は、アソシエーション拒否のアソシエーション応

答メッセージを移動局ＭＴ１に送信する。なお、ここでのＷＥＰのアルゴリズムは、ＲＳＡ Ｄａｔａ Ｓｅｃｕｒｉｔｙ Ｉｎｃ．のＲＣ４技術により規定されている。

【００１２】

つまり、この認証方法によれば、アクセスポイントと移動局が、あらじめ、秘密のＫｅｙであるＳｈａｒｅｄ Ｓｅｃｒｅｔ Ｋｅｙを持ち合うことで、アクセスポイントが特定の移動局への認証／アソシエーションを許可する仕組みを実現している。ここで、移動局側は、本Ｓｈａｒｅｄ Ｓｅｃｒｅｔ Ｋｅｙを、一般ユーザから、読み取れない実装形態にし、悪意を持った侵入者からの盗難（読み取り）を防ぎ、本Ｋｅｙ自体が無線伝送路を行き交うことがないので、傍受されることもなく、ある程度のセキュリティレベルを確保している。

【００１３】

【発明が解決しようとする課題】

しかしながら、このような従来のアクセスポイント装置の認証処理方法にあっては、認証のためのアルゴリズムと、その認証のためのＫｅｙが、悪意を持ってネットワークに侵入しようとする者に、不正に盗まれることがないという前提でのセキュリティの確保であり、この前提は１００％担保できるものではない。すなわち、正式手順によってアクセスポイントに、認証可能な端末の全くのコピーが、作られないという保証はなく、また、そのユーザからアクセスできないメモリに、格納されているＫｅｙが、特殊な機器を使うことで、不正に読み取られる可能性もないとは言いきれない。よって、これらの不正な行為によって、悪意を持ってネットワークに、侵入しようとする者が、ある端末を不正にアソシエーションすることができれば、有線のケーブル接続のような物理的な作業なしに、アクセスポイントのカバーするエリアであれば、物理的に、隠れてネットワークに侵入することができる。つまり、ある閉じられた空間（オフィスや、家庭）内で、ワイヤレスネットワークを構築した場合で、その中心にあるアクセスポイントのカバーするエリア内であれば、その閉じられた区間の外部、つまり、壁等で隔てられた死角にある、悪意を持ってネットワークに侵入しようとする者の端末からのアソシエーションを許してしまう可能性があるという問題があった。

【００１４】

本発明は、このような課題に鑑みてなされたものであって、ワイヤレスＬＡＮシステムにおいて、セキュリティレベルを飛躍的に向上させることができるアクセスポイント装置及びその認証処理方法を提供する。

【００１５】

【課題を解決するための手段】

本発明のアクセスポイント装置は、有線伝送路で構築されるネットワークとのインターフェース機能を備え、無線ＬＡＮエリア内で複数の移動局とデータリンク接続を

行うアクセスポイント装置において、複数の移動局とのデータリンク確立を行うためのアソシエーション手順と認証手順を実行する認証／アソシエーション実行手段と、前記エリア内の移動局が、前記アソシエーション手順を開始する前に前記認証手順を行おうとする場合に、前記ＬＡＮを管理するネットワーク管理者に対し、認証手順の最終的な許可を得るために、認証を求めている移動局がいることを通知する通知手段と、前記通知を受けた前記ネットワーク管理者による、前記認証を求めている移動局に対しての認証の許可又は拒否の指示が入力される入力手段と、を備えることを特徴とする。

【００１６】

本発明のアクセスポイント装置の認証処理方法は、有線伝送路で構築されるネットワークとのインターフェース機能を備え、無線ＬＡＮエリア内で複数の移動局とデータリンク接続を行うアクセスポイント装置の認証処理方法において、前記移動局から前記アクセスポイント装置への認証要求により、前記移動局及び前記アクセスポイント装置が、所定の認証手続を開始する第１ステップと、前記認証手続により、前記アクセスポイント装置が、前記移動局への認証を許可しようとするとき、前記認証手続における最終メッセージである認証応答メッセージを前記移動局に返信する前に、前記ＬＡＮを管理するネットワーク管理者に対して、前記認証手順の最終的な許可を通知するとともに、最終認証が行われるまでの最大待ち時間を設定した認証待ちタイマをスタートさせる第２ステップと、前記ネットワーク管理者が、前記アクセスポイント装置に対して、前記認証待ちタイマがタイムアウトする前に、最終の認証の許可又は拒否を指示する第３ステップと、前記ネットワーク管理者により、前記認証待ちタイマがタイムアウトする前に、最終の認証許可が指示されると、前記アクセスポイント装置が、前記認証応答メッセージを、認証許可として前記移動局に返信する第４ステップと、前記認証応答メッセージを受信した前記移動局が、アソシエーションの手順を開始する第５ステップと、を実行することにより前記移動局の認証が完了し、アソシエーション手順を開始することを特徴とする。

【００１７】

また、前記第３ステップでは、前記ネットワーク管理者が、認証を拒否する指示を前記アクセスポイント装置に指示した場合に、前記認証手続における最終メッセージである認証応答メッセージを、認証拒否として前記移動局に返信するものであってもよい。

【００１８】

また、前記第３ステップでは、前記ネットワーク管理者が、認証を拒否又は許可する指示を前記アクセスポイント装置に指示する前に、前記認証待ちタイマがタイムアウトすると、前記認証手続における最終メッセージである認証応答メッセージを、認証拒否として前記移動局に

返信するものであってもよい。
また、好ましい具体的な態様としては、前記認証手続は、ＩＥＥＥ８０２．１１が規定するＳｈａｒｅｄ Ｋｅｙ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ手順であってもよい。

【００１９】

【発明の実施の形態】

以下、添付図面を参照しながら本発明の好適なアクセスポイント装置及びその認証処理方法の実施の形態について詳細に説明する。
図１は、本発明の実施の形態のアクセスポイント装置の概略構成を示す図である。

【００２０】

本実施の形態のアクセスポイント装置１８は、前記図５のアクセスポイントＡＰ２に置き換えて設置される。すなわち、前記図５において、ある有線伝送路により実現される、他ネットワーク７に接続された、アクセスポイントＡＰ２と、そのＡＰ２がカバーする、有限なエリアに存在する移動局ＭＴ１、ＭＴ２、ＭＴ３、ＭＴ４から構成される、ワイヤレス・エリア・ネットワーク１において、前記アクセスポイントＡＰ２は、図１に示すアクセスポイント装置１８に置き換えて構成される。

【００２１】

図１において、アクセスポイント装置１８は、複数の移動局ＭＴ１、ＭＴ２、ＭＴ３、ＭＴ４との無線接続を実現するために、無線変復調部、ベースバンド信号処理部及びデータリンク制御部からなる無線通信処理手段１２と、無線通信処理手段１２に接続される無線送受信用のアンテナ１９と、他ネットワーク７と任意の有線伝送路１７によりデータリンク接続し、無線通信処理手段１２により送受信されるデータをインターフェースする機能を実現するネットワークインターフェース手段１４と、無線通信処理手段１２が、複数の移動局とのデータリンク確立を行うためのアソシエーション手順と認証手順を実行し、そこで、必要になる、移動局ＭＴ１、ＭＴ２、ＭＴ３、ＭＴ４と交換される制御メッセージを無線通信処理手段１２とやりとりする機能を実現する認証／アソシエーション処理手段１３と、認証／アソシエーション処理手段１３が、認証処理を行う場合に、最終的にそれを許可し、認証許可すべき移動局に認証許可のメッセージを送信する前に、それを通知することで、ワイヤレス・エリア・ネットワーク１を管理するユーザに、表示デバイスやスピーカ等で認証要求している移動局の存在を通知する機能を実現する認証要求表示手段１６（通知手段）と、認証要求表示手段１６により認証要求している移動局の存在が通知された後に、ワイヤレス・エリア・ネットワーク１を管理するユーザが、それを許可又は拒否することを、認証／アソシエーション処理手段１３に通知するためにボタン等の人間の物理的な入力を受け付ける機能を実現する認証入力手段１５（入力手段）とから構成される。

【００２２】

以下、上述のように構成されたアクセスポイント装置の認証処理方法の動作を説明する。
ここでは、ある移動局が、電源投入等の動作により、認証処理手順とアソシエーション処理手順が実行され、アクセスポイント装置１８とのデータリンク接続が確立される場合と認証が拒否される場合のシーケンスを説明する。

【００２３】

前記図５における移動局ＭＴ１を、認証処理を行う対象の移動局とし、移動局ＭＴ２、ＭＴ３、ＭＴ４は、既にアクセスポイント装置１８とアソシエーションまで完了し、データリンクが確立しているものとする。
まず、移動局ＭＴ１が、認証手続きにより、ネットワークを管理するユーザが、その認証を許可し、その後、アソシエーション手続きにより、アクセスポイント装置１８とのデータリンクが確立される場合を、図２及び図４を参照して説明する。

【００２４】

図２は、認証許可の場合の認証手順の制御シーケンスを示す図である。
移動局ＭＴ１が、電源投入等の動作により、まず、Ｓｈａｒｅｄ Ｋｅｙ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ方法による認証手続きを開始するための認証要求メッセージ１をアクセスポイント装置１８に送信する。

【００２５】

アクセスポイント装置１８において、無線通信処理手段１２を介して、このメッセージを受信した認証／アソシエーション処理手段１３は、ＡＰ認証処理１（図２の番号２０参照）として、この認証手続きの度に、任意に決めることができる、Ｉｎｉｔｉａｌｉｚａｔｉｏｎ ＶｅｃｔｏｒとＳｅｃｒｅｔ Ｋｅｙの値をパラメータとし、ＷＥＰ（Ｗｉｒｅｄ Ｅｑｕｉｖａｌｅｎｔ Ｐｒｉｖａｃｙ）ＰＲＮＧ（Ｐｓｅｕｄｏｒａｎｄｏｍ Ｎｕｍｂｅｒ Ｇｅｎｅｒａｔｏｒ）のアルゴリズムに従い数値演算を行い、１２８０ｃｔｅｔの一意に決まるＣｈａｌｌｅｎｇｅ Ｔｅｘｔの値を算出し、この値を含めた認証応答メッセージ１を無線通信処理手段１２を介して移動局ＭＴ１に送信する。

【００２６】

次に、ＭＴ認証処理２１として、本認証応答メッセージ１を受信した、移動局ＭＴ１は、その中に含まれるＣｈａｌｌｅｎｇｅ Ｔｅｘｔの値を、ＷＥＰの暗号化アルゴリズムに従い、Ｓｈａｒｅｄ Ｓｅｃｒｅｔ ＤａｔａとＩｎｉｔｉａｌｉｚａｔｉｏｎ Ｖｅｃｔｏｒをパラメータにして暗号化を行い、その値をＩｎｉｔｉａｌｉｚａｔｉｏｎ Ｖｅｃｔｏｒと共に、認証要求メッセージ２に含めてアクセスポイント装置１８に返信する。
さらに、アクセスポイント装置１８において、無線通信

処理手段１２を介して、このメッセージを受信した認証／アソシエーション処理手段１３は、ＡＰ認証処理２（図２の番号２２参照）として、受信した暗号化されたＣｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を、同時に受信したＩｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒと予め知っているＳｈａｒｅｄ　Ｓｅｃｒｅｔ　Ｄａｔａを基にデコードし、その結果と前述の元のＣｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を比較し、それが同一であれば、ＡＰ認証処理３（図２の番号２３参照）の手順を実行する。この手順を示したのが図４に示すフローのステップＳ３０～ステップＳ３３の処理である。

【００２７】

図４は、上記アクセスポイントの認証処理を示すフローチャートである。

まず、この手順においては、アクセスポイント装置１８の認証／アソシエーション処理手順１３は、認証要求表示手段１６に対して、認証待ちであることを通知し（ステップＳ３０）、それと同時に、任意の時間に設定された認証待ちタイマをスタートさせ（ステップＳ３１）、認証入力待ち（ステップＳ３２）の状態に入る。一方、認証待ちであることの通知を受けた、認証要求表示手段１６は、直ぐに、ネットワークを管理するユーザに対して表示デバイスやスピーカ等で認証要求している移動局が存在することを通知する。

【００２８】

ここで、認証／アソシエーション処理手順１３は、認証待ちタイマがタイムアウトする前に認証入力手段１６からのネットワークを管理するユーザの認証許可の入力による認証許可入力の通知を受ければ、認証許可を示した認証応答メッセージ２を無線通信処理手段１２を介して移動局ＭＴ１に送信する（ステップＳ３３）。

【００２９】

図２に戻って、本認証応答メッセージ２を受信した移動局ＭＴ１は、その結果が、許可であることから、次のアソシエーションの手順に入り、アソシエーション要求メッセージを、アクセスポイント装置１８へ送信する。

【００３０】

ここで、アクセスポイント装置１８においては、無線通信処理手段１２を介して、このメッセージを受信した認証／アソシエーション処理手段１３は、アソシエーション処理（図２の番号２４参照）として、アソシエーション要求メッセージ中のＳＳＩＤ（Ｓｅｒｖｉｃｅ　Ｓｅｔ　Ｉｄｅｎｔｉｆｉｅｒ）にて、移動局ＭＴ１を識別し、予め決められたアソシエーション許可ルールに従い、そのアソシエーションを許可するかどうかを決定し、それを許可するときは、無線通信処理手段１２を介して移動局ＭＴ１へアソシエーション許可を示したアソシエーション応答メッセージを送信する。このアソシエーション応答メッセージを移動局ＭＴ１が受信すれば、移動局ＭＴ１とアクセスポイント装置１８の間でデータ

リンクが確立され、以降、データの通信が可能になる。

【００３１】

次に、移動局ＭＴ１が、認証手続きにおいて、ネットワークを管理するユーザにより、その認証を拒否される場合、及び、認証待ちタイマがタイムアウトして、自動的に、認証が拒否される場合を図３及び図４を参照して説明する。

【００３２】

図３は、認証拒否／タイムアウト場合の認証手順の制御シーケンスを示す図である。

図３において、移動局ＭＴ１が、電源投入等の動作により、Ｓｈａｒｅｄ　Ｋｅｙ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ方法による認証手続きを開始するための認証要求メッセージ１をアクセスポイント装置１８に送信する。

【００３３】

アクセスポイント装置１８において、無線通信処理手段１２を介して、このメッセージを受信した認証／アソシエーション処理手段１３は、ＡＰ認証処理１（図３の番号２５参照）としてこの認証手続きの度に、任意に決めることができる、Ｉｎｉｔｉａｌｉｚａｔｉｏｎ　ＶｅｃｔｏｒとＳｅｃｒｅｔ　Ｋｅｙの値をパラメータとし、ＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）ＰＲＮＧ（Ｐｓｅｕｄｏｒａｎｄｏｍ　Ｎｕｍｂｅｒ　Ｇｅｎｅｒａｔｏｒ）のアルゴリズムに従い数値演算を行い、１２８０ｃｔｅｔの一意に決まるＣｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を算出し、この値を含めた認証応答メッセージ１を、無線通信処理手段１２を介して、移動局ＭＴ１に送信する。

【００３４】

次に、ＭＴ認証処理（図３の番号２６参照）として、本認証応答メッセージ１を受信した移動局ＭＴ１は、その中含まれるＣｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を、ＷＥＰの暗号化アルゴリズムに従い、Ｓｈａｒｅｄ　Ｓｅｃｒｅｔ　Ｄａｔａと、Ｉｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒをパラメータに暗号化を行い、その値をＩｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒと共に、認証要求メッセージ２に含めてアクセスポイント装置１８に返信する。さらに、アクセスポイント装置１８において、無線通信処理手段１２を介して、このメッセージを受信した認証／アソシエーション処理手段１３は、ＡＰ認証処理２（図３の番号２７参照）として受信した暗号化されたＣｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を、同時に受信したＩｎｉｔｉａｌｉｚａｔｉｏｎ　Ｖｅｃｔｏｒと予め知っているＳｈａｒｅｄ　Ｓｅｃｒｅｔ　Ｄａｔａを基にデコードし、その結果と前述の元のＣｈａｌｌｅｎｇｅ　Ｔｅｘｔの値を比較し、それが同一であればＡＰ認証処理３（図３の番号２８参照）の手順を実行する。この手順を示したのが図４に示すフローのステップＳ３０～ステップＳ３２、ステップＳ３４の処理である。

13

【００３５】
まず、この手順においては、アクセスポイント装置１８の認証／アソシエーション処理手順１３は、認証要求表示手段１６に対して認証待ちであることを通知し（ステップＳ３０）、それと同時に、任意の時間に設定された認証待ちタイマをスタートさせ（ステップＳ３１）、認証入力待ち（ステップＳ３２）の状態に入る。一方、認証待ちであることの通知を受けた認証要求表示手段１６は、直ぐに、ネットワークを管理するユーザに対して表示デバイスやスピーカ等で認証要求している移動局が存在することを通知する。

【００３６】
ここで、認証／アソシエーション処理手順１３は、認証待ちタイマがタイムアウトする前に認証入力手段１６からのネットワークを管理するユーザの認証拒否の入力による認証拒否入力の通知を受ければ、認証拒否を示した認証応答メッセージ２を無線通信処理手段１２を介して移動局ＭＴ１に送信する（ステップＳ３４）。同様に、認証入力待ち（ステップＳ３２）の状態において、認証待ちタイマがタイムアウトすれば、認証拒否を示した認証応答メッセージ２を無線通信処理手段１２を介して移動局ＭＴ１に送信する（ステップＳ３４）。

【００３７】
図３に戻って、本認証応答メッセージ２を受信した移動局ＭＴ１は、その結果が拒否であることから次のアソシエーションの手順には入れず、必要があれば、ユーザに対して認証が失敗したことを通知する（図３の番号２９参照）。よって、この場合は、移動局ＭＴ１は、データ通信を行うことができない。

【００３８】
なお、ここで言及している、ＷＥＰのアルゴリズムは、ＲＳＡ Ｄａｔａ Ｓｅｃｕｒｉｔｙ Ｉｎｃ．のＲＣ４技術により規定されており、また、アソシエーション処理（図２の番号２４参照）も、ＩＥＥＥ８０２．１１で規定されるアソシエーション手順と同一であることとする。

【００３９】
また、ここでの認証待ちタイマに設定されている任意の時間とは、ネットワークを管理するユーザが、認証要求表示手段により、認証待ちの移動局が存在することを認識してから、それを許可するために、認証入力手段により、許可の入力をするまでに必要な時間から換算される妥当な値として、ネットワークを管理するユーザが、任意に設定可能であるものとする。

【００４０】
以上述べたように、本実施の形態では、アクセスポイント装置１８は、エリア内の移動局が、アソシエーション手順を開始する前に認証手順を行う場合に、アクセスポイント装置１８が、ＬＡＮを管理するネットワーク管理者に対し、認証手順の最終的な許可を得るために、認証

14

を求めている移動局がエリア内にいることを通知する認証要求表示手段１６と、通知を受けたネットワーク管理者が、認証を求めている移動局に対して認証の許可又は拒否を指示する認証入力手段１５とを備え、物理的に目視できないがために、悪意を持った、ネットワークへの侵入者の攻撃を受けやすい、ワイヤレスＬＡＮシステムにおいて、移動局のアソシエーション前の認証手続きで、アクセスポイントがそれを許可することを自動的に行わず、そのネットワークを管理するユーザが、誰がアソシエーションしようとしているのかを目視した上で、その許可を与えることができるので、セキュリティレベルを飛躍的に向上させることができる。

【００４１】
また、この認証の手順は、ＩＥＥＥ８０２．１１で、オプションとして規定されている、Ｓｈａｒｅｄ Ｋｅｙ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ手順を実装しているワイヤレスＬＡＮシステムにおいては、アクセスポイント装置についてのみ追加の実装が必要であり、移動局装置は、なんら変更をすることなく機能させることが可能である。

【００４２】
【発明の効果】
以上、詳述したように、本発明によれば、ワイヤレスＬＡＮシステムにおいて、セキュリティレベルを飛躍的に向上させることができ、また、移動局装置は、なんら変更をすることなく実施することができる。

【図面の簡単な説明】
【図１】本発明の実施の形態のアクセスポイント装置の概略構成を示す図である。
【図２】本実施の形態のアクセスポイント装置の認証許可の場合の認証手順の制御シーケンスを示す図である。
【図３】本実施の形態のアクセスポイント装置の認証拒否／タイムアウト場合の認証手順の制御シーケンスを示す図である。
【図４】本実施の形態のアクセスポイント装置のアクセスポイントの認証処理を示すフローチャートである。
【図５】従来のワイヤレスＬＡＮシステムの概略構成を示す図である。
【図６】従来のワイヤレスＬＡＮシステムの認証手順とアソシエーション手順の制御シーケンスを示す図である。

【符号の説明】
１　ワイヤレス・エリア・ネットワーク
３　移動局ＭＴ１
４　移動局ＭＴ２
５　移動局ＭＴ３
６　移動局ＭＴ４
７　他ネットワーク
１２　無線通信処理手段
１３　認証／アソシエーション処理手段

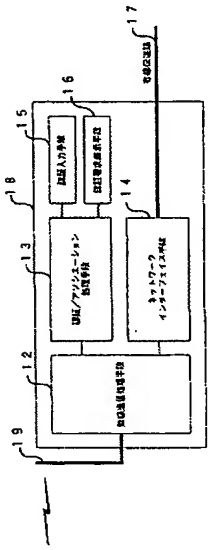
15

１４　ネットワークインターフェース手段
１５　認証入力手段（入力手段）
１６　認証要求表示手段（通知手段）

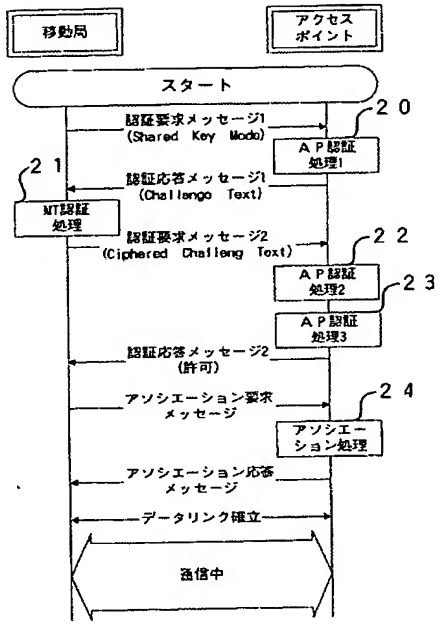
16

１７　有線伝送路
１８　アクセスポイント装置
１９　無線送受信用のアンテナ

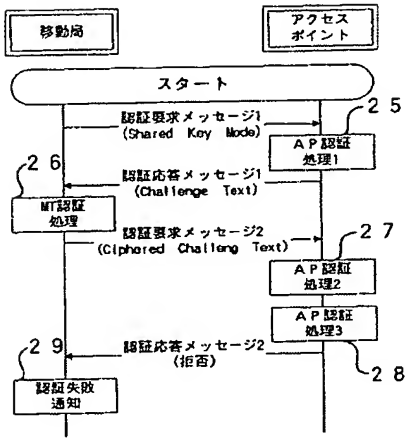
【図１】



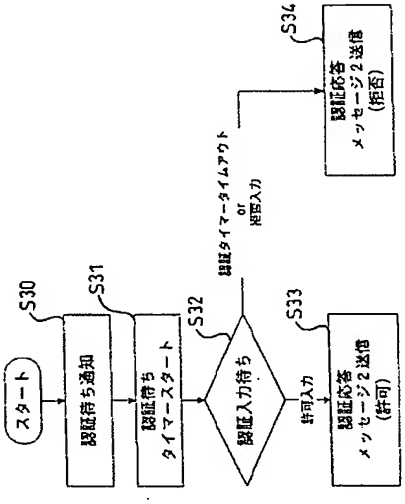
【図２】



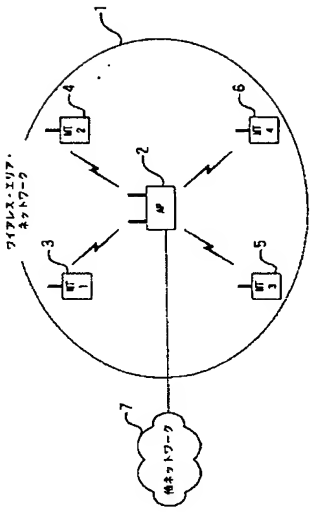
【図３】



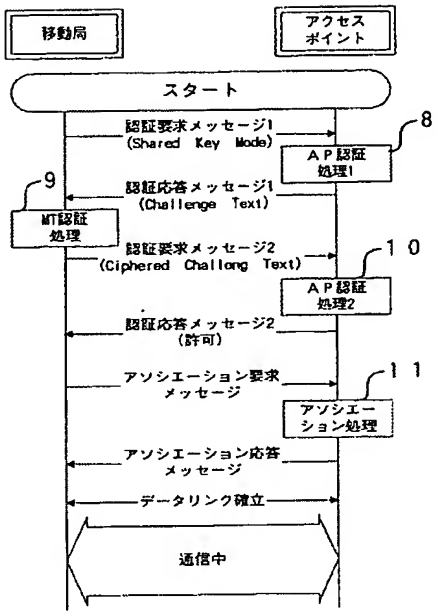
【図４】



【図５】



【図６】



フロントページの続き

(56)参考文献　特開平１０－０７０５４０（ＪＰ，Ａ）
特開２０００－００３３３６（ＪＰ，Ａ）
A. R. Prasad et al., Security architecture for wireless LANs: corporate & public environment, Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st, ２０００年　５月１８日, Vol. 1, pp. 283-287

(58)調査した分野(Int.Cl.[7], ＤＢ名)
H04L 12/28　300
H04L　9/32
H04Q　7/38